FORSCHUNGSZENTRUM JÜLICH GmbH

Jülich Supercomputing Centre

D-52425 Jülich, Tel. (02461) 61-6402

Interner Bericht

IPv6 Testbed im JSC

Werner Anrath, Egon Grünter, Sabine Werner

FZJ-JSC-IB-2011-05

Oktober 2011

(letzte Änderung: 07.10.2011)

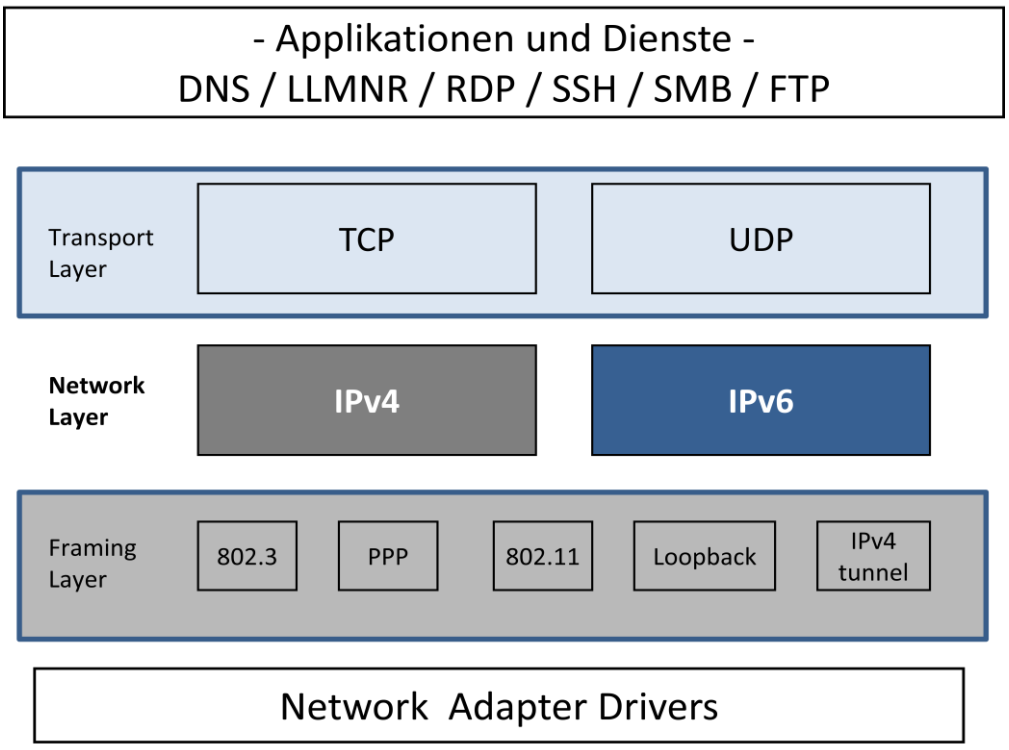
Inhalt

IPv6 Status 2011

Im Jahr 1995 wurde von der Internet Engineering Task Force (IETF) IPv6 als Nachfolgetechnik des allgegenwärtigen IPv4-Protokolls ausgewählt.

Durch die Knappheit der IPv4-Adressen und die Zuweisung der letzten freien IPv4 Adressblöcke durch die Internet Assigned Numbers Authority (IANA) im Frühjahr 2011 hat das IPv6-Protokoll an Bedeutung gewonnen. Seit 2006 bietet der Verein zur Förderung eines Deutschen Forschungsnetzes (DFN Verein) den angeschlossenen Einrichtungen im Wissenschaftsnetz (X-WiN) native IPv6 Regelbetrieb an. Verliefen diese Vorbereitungen seitens der Provider und die Einführung von IPv6 in den Transportnetzen eher unbemerkt, änderte sich die Situation in den lokalen Netzen zunehmend. Mit der Einführung von Windows Vista und den Windows-Server-Plattformen im Jahr 2007 ist das IPv6-Protokoll installiert und aktiv.

Mit der Ablösung der Windows XP Systeme durch Windows 7 wird aktuell die Verbreitung des IPv6 Protokolls gesteigert. Neben den Microsoft-Betriebssystemen nutzen auch die bekannten LINUX-Varianten und Mac OS X das neue IPv6 Protokoll parallel zum etablierten IPv4-Protokoll. Die Netzwerkadministratoren im lokalen Netz sind dadurch zum Handeln gezwungen. Wesentlich ist dabei, dass dieses neue Protokoll in den unterschiedlichen Betriebssystemen installiert und standardmäßig aktiviert ist, so dass die Systeme im Dual-Stack-Betrieb (siehe Grafik) am Netzwerk kommunizieren. Die Microsoft-Betriebssysteme nutzen zudem sogenannte Transition Technologies, die den Zwang zur Planung und Organisation des IPv6-Betriebs im lokalen Netz erhöhen.



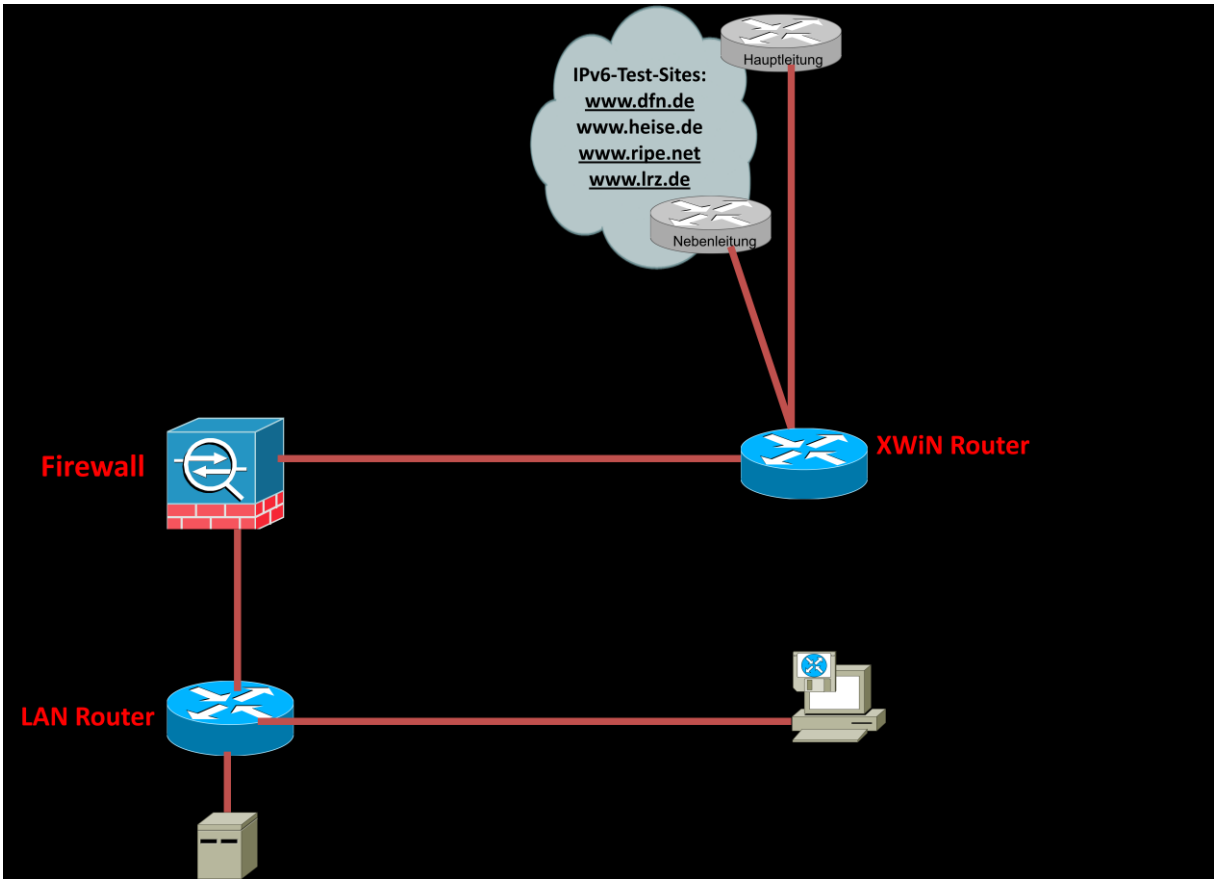
IPv6 – Dual Stack Implementierung

Ziele – IPv6 Testbed im JSC

Im IPv6 Testbed des JSC sollen die bis März 2011 gewonnen Erfahrung aus Labortests und bisherige konzeptionelle Planungsarbeiten zusammengeführt werden. Die Umsetzbarkeit derselben sollten in einer Produktionsumgebung durch einen Core-to-Edge Ansatz nachgewiesen werden. Dieser Ansatz wurde gegenüber den Varianten Edge-to-Core oder der Migration einzelner Bereiche als IPv6-Inseln bevorzugt, da kein Zwang zur Migration durch eine etwaige Adressknappheit besteht und damit gegenwärtig die Komplexität am besten beherrschbar ist.

Ausgehend von diesem Core-to-Edge Ansatz wurden folgende fünf Phasen zur Umsetzung durchlaufen:

- Phase 1 - WAN-Anbindung, Firewall, LAN-Routing
- Phase 2 - Client-Netz (Abt. JSC-KS)
- Phase 3 - Client-Netz (JSC weit, ca. 400 Systeme)
- Phase 4 - Server-Netz (File-Server, Terminal-Server)
- Phase 5 - Fazit - IPv6 Zukunft im Forschungszentrum



Topologie IPv6 Testbed

Zunächst werden in den folgenden Abschnitten die Planungen und Vorüberlegungen dargestellt. Anschließend werden die Phasen im Detail technisch erörtert und Erfahrungen vorgestellt. Grundlegende Kenntnisse über IPv6-Adressierung, -Konfiguration und -Routing werden dabei vorausgesetzt und sind unabdingbar für das Verständnis der in diesem Bericht dargestellten Zusammenhänge. Zur Einführung in die Thematik eignen sich die in [1] und [2] genannten Werke.

WAN und LAN Umgebung

Die Internet-Anbindung des Forschungszentrum Jülichs ist über eine redundante Verbindung zum X-WiN realisiert. Im Backup-Fall wird mittels Border-Gateway-Protokoll-Routing (BGP) automatisch auf die Ersatzleitung umgeschaltet und die IPv4-Konnektivität bleibt bestehen. Der DFN-Verein bietet seit 2006 den angeschlossenen Einrichtungen native IPv6-Konnektivität an, wobei Bandbreitenverteilung und Redundanzkonzept identisch mit dem etablierten IPv4 Angebot sind. Im Herbst 1999 erhielt der DFN Verein von RIPE[1] den Prefix 2001:638::/32 zugewiesen. Im Jahr 2002 hat das JSC für das Forschungszentrums Jülich den IPv6-Prefix 2001:638:404::/48 offiziell registrieren lassen. Im Frühjahr 2011 konnte im Rahmen des hier beschriebenen Testbeds erstmals mittels IPv6 Kommunikation auf externe Inhalte zugegriffen werden. Seit dem Beginn der IPv4 Ära 1990 im Forschungszentrum Jülich ist damit ein neues Netzwerkprotokoll auch für die externe Kommunikation betriebsbereit.

Der Übergang in die LAN-Umgebung ist durch eine leistungsfähige redundante Firewall-Konfiguration geschützt, die sowohl IPv4 als auch IPv6 Verkehr effizient reglementieren kann.

Die LAN-Umgebung im Forschungszentrum Jülich besteht aus einer Vielzahl verschiedener Subnetze, in denen die angeschlossenen Systeme jeweils mit festen IPv4-Adressen ausgestattet sind; diese werden entweder manuell oder mittels Dynamic Host Configuration Protocol (DHCP) konfiguriert.

Bedingt durch stetiges Wachstum und Reorganisation einzelner Forschungsbereiche unterscheiden sich die Subnetze stark in der Anzahl der angeschlossenen Systeme wie auch in der Strukturierung nach Aufgaben.

Lediglich in Wireless LAN- und Access-VPN[2]-Netzen wird mit Adress-Pools und dynamischer Zuweisung gearbeitet. Die Verwaltung der Netzwerkparameter erfolgt datenbankgestützt. So werden z.B. sämtliche Daten für den DNS[3]- und DHCP-Betrieb direkt aus Inhalten der Datenbank generiert. Die installierten DHCP Server ordnen den in der zentralen Datenbank verwalteten MAC-Adressen [4] jeweils fest eine IPv4-Adresse aus dem IPv4 Class-B-Netz zu. Die DNS-Server unterstützen Forward- und Reverse-Lookup. Dynamisches DNS ist nicht nötig, da alle Ressource-Records direkt aus Inhalten der zentralen Datenbank generiert werden können.

Durch Zulauf aktueller Switching-Hardware mit erweiterter IPv6-Funktionalität verbessern sich aus Sicht des Netzwerkmanagements die Möglichkeiten IPv6 betriebssicher anbieten zu können und den IPv4-Betrieb der Dual-Stack-Systeme stabil zu halten.

[1] Réseaux IP Européens Network Coordination Centre (RIPE NCC)
[2] Virtual Private Network
[3] Domain Name System
[4] 48 Bit Ethernet Adresse

IPv6 Adressplanung Netzwerk

Eine IPv6-Adressplanung ist obligatorisch und sollte möglichst optimal an die vorhandenen Management-Instrumente und Datenbankinhalte anknüpfen, aber gleichzeitig offen für zukünftige reine IPv6 Umgebungen sein. Der Zusatzaufwand, personell und finanziell, sollte letztlich überschaubar sein, da kein unmittelbarer Zwang besteht, kurzfristig Dienste auf IPv6 Basis anbieten zu müssen und auch kein Mangel an IPv4-Adressen im lokalen Netz vorliegt.

Anknüpfend an die Ausführungen zur IPv4-Adressierung, den Datenbankinhalten und etablierten Prozessen im Netzwerkmanagement sollte sowohl die Möglichkeit zur festen IPv6 Adressierung als auch zur automatischen Konfiguration gegeben sein. Die automatische Konfiguration reduziert den Konfigurationsaufwand und minimiert das Risiko für fehlerhafte Eingaben. Die Zuteilung der IPv6-Netzwerk-Prefixe soll einer einheitlichen Konvention folgen, die auch optional eine Verknüpfung mit der IPv4-Subnetzadresse zulässt. Aufgrund des erwarteten langfristigen Parallel-Betriebs beider Netzwerk-Protokolle werden IPv4 und IPv6-Subnetze deckungsgleich betrieben.

Einerseits kann durch manuelles Eintragen einer fest vorgegebenen IPv6-Adresse ein System dauerhaft die gleiche IPv6-Adresse führen und mittels DNS AAAA-Records benutzerfreundlich im Netzwerk erreicht werden. Andererseits kann durch entsprechende Signalisierung im Router Advertisement effizient für alle Hosts in einem Subnetz eine Autokonfiguration initiiert werden. Dabei verteilt der Router das Subnetz-Prefix und die Hosts generieren dazu einen eindeutigen Interface Identifier (IID) der zusammen mit dem Netzwerkprefix die 128 Bit IPv6 Adresse bildet.

Die Adressierung der IPv6 Subnetze kann die IPv4 Subnetz-Adresse übernehmen; dazu stehen 16 Bit im IPv6-Prefix zur Verfügung; die restlichen Bits werden mit Null aufgefüllt. Auf jeden Fall soll das Konzept konform zu ‚RFC5375[5] – IPv6 Unicast Address Assignment Considerations' sein.

Das folgende Beispiel konkretisiert die Überlegungen. Im bisherigen IPv4-Subnetz 134.94.160.0/21 soll Dual-Stack-Betrieb ermöglicht werden. Die Beziehung zwischen den Subnetzadressen soll für die Netzwerkadministratoren leicht nachvollziehbar sein:

IPv4-Netzadresse: 134.94.**160**.0/24 , d.h. 8 Bit für die Adressierung von Endsystemen

IPv6-Netz: 2001:638:404:**A0**00::/64 , d.h. 64 Bit für die Adressierung von Endsystemen

Für den zentralen Router ergeben sich daraus z.B. folgende IPv6 Adressen:

134.94.160.1/24	**IPv4 Adresse**
2001:638:404:A000::A000:1	**zentraler Router (Global)**
fe80::A000:1	**zentraler Router (Link Local)**

Weitere (auch reine) IPv6-Subnetze sind in Zukunft möglich: 2001:0638:0404:A001::/64

2001:0638:0404:A002::/64

[5] Request for Comments

Die Adressierung reiner Transportnetze zwischen zwei Routern ohne angeschlossene Hosts soll zur Illustration als weiteres Beispiel für CISCO IOS[6] gezeigt werden und die Transformation verdeutlichen:

```
interface Vlan801
    ip address 134.94.111.181 255.255.255.248
    ipv6 address FE80::6FB0:5 link-local
    ipv6 address 2001:638:404:6FB0::6FB0:5/64
    ipv6 nd ra suppress
```

Hier werden die Global IPv6 Unicast Address und die IPv6 Link Local Address manuell konfiguriert. Im Gegensatz zu einem Host startet ein Router-Interface keinen Autokonfigurationsprozess (RFC 2462). Die Hex-Kombination 6FB0 entspricht dem extrahierten IPv4-Subnetzanteil aus 134.94.111.176/29 und 5 ist die Nummerierung im Subnetz analog zu IPv4. Aus Gründen der Übersichtlichkeit, insbesondere bei der Fehlersuche, wird der Subnetzanteil im IID[7] wiederholt. Also ergibt das den IID ::6FB0:5, der mit dem vorangestellten Prefix die IPv6-Adresse 2001:638:404:6FB0::6FB0:5 bildet und direkt mit der IPv6 Link-Local-Address korrespondiert.

Die hier im Beispiel gezeigte Syntax kann sowohl auf CISCO IOS als auch zur Konfiguration von IPv6 Verbindungen auf der ASA Firewall Anwendung finden.

Bisherige und neue Experiment-Netze mit privaten IPv4-Adressen (RFC1918) werden als Unique Local Address (ULA) nach RFC 4193 geführt und können im Intranet-Routing integriert werden:

IPv4: private Adressen (z.B. 192.168.6.0/24)

IPv6: Unique Local Address, d.h. Prefix FD00::/7

IPv6 im LAN / Adressierung der Hosts

Zentrale Server in eigenen Subnetzen oder DMZs[8] sowie Router werden manuell konfiguriert und erhalten wie oben gezeigt feste Adressen, die beim Dual Stack Betrieb durch Transformation die vorhandene IPv4 Nummerierung aus der zentralen Netzwerkdatenbank beinhalten. Bei reinem IPv6 Betrieb ist die Nummerierung in Zukunft gesondert zu erzeugen.

2001:638:404:5000::5000:2 DNS Server, manuelle Konfiguration (Global)

2001:638:404:6900::6900:5 File Server, manuelle Konfiguration (Global)

Wichtig ist hierbei, dass die Router Advertisements in diesen Subnetzen kein Flag für die Autokonfiguration enthalten (RFC 2462). Ansonsten würden die Systeme mit mehreren Global Unicast Adressen aktiv. Zur Verdeutlichung hier eine entsprechende Cisco IOS Router-Konfiguration:

[6] Internetwork Operating System
[7] Interface Identifier (IPv6)
[8] Demilitarized Zone

interface Vlan14
description IPv6 Server Address SUBNET - NO AUTOCONFIG
ip address 134.94**.105**.*48* 255.255.255.0
ipv6 address FE80::6900:30 link-local
ipv6 address 2001:638:404**:69**00*::69*00:*30*/64
ipv6 nd prefix 2001:638:404:6900::/64 2592000 604800 **no-autoconfig**
!!! Stateless Address Autoconfiguration OFF
ipv6 nd ra suppress

In anderen Subnetzen mit überwiegend Arbeitsplatzsystemen ist Stateless Address Autoconfiguration sinnvoll. DHCPv6 ist zwar als Standard verfügbar, jedoch ist die Integration insbesondere im LINUX-Bereich nicht ausgereift, siehe Anhang IPv6 Tests im JSC Labor. Bezogen auf die Betriebssicherheit wiegen sich die Nach- und Vorteile im Vergleich zur Stateless Address Autoconfiguration auf. Anmerkung: Die Zuweisung fester IPv6-Adressen mittels DHCPv6 (RFC 3315) setzt die Erfassung eines 14 Byte langen DHCP Unique Identifiers (DUID) voraus, der vom Host beim ersten Start erzeugt wird. Dieser DUID ist zur Konfiguration eines DHCPv6-Server zentral zu verwalten, um feste IIDs zuweisen zu können. Die in der IPv4-Welt bekannte Zuordnung über die MAC-Adresse als Client-Identifier existiert nicht.
Die Absicherung gegen Rogue DHCPv6-Server muss ebenfalls gewährleistet werden.

Sofern die automatische Konfiguration durch Stateless Address Autoconfiguration erfolgt, kann der aus der Ethernet-MAC-Adresse (48 Bit) abgeleitete Interface Identifier (IID) entsprechend dem EUI-64[9] Standard ebenfalls als fest angesehen werden. DNS-Einträge und Traffic Filter können an diese Konvention anknüpfen, da die MAC-Adressen in der zentralen Netzwerkdatenbank bekannt sind und diese durch die EUI-64 Transformation in die IPv6-Adresse als IID eingehen.

2001:0638:0404:A80:: eui-64 USER PCs Stateless Autoconfiguration (Global)

fe80:: eui-64 USER PCs Stateless Autoconfiguration (Link Local)

Konkret ergeben sich aus der MAC-Adresse (48 Bit)

00:15:77:96:74:bc

durch Einfügen von **ff:fe** zwischen Hersteller-ID und Board-ID

00:15:77:**ff:fe**:96:74:bc

und invertieren des **U/L-Bit** entsprechend dem IEEE EUI-64 Standard

0**2**:15:77:ff:fe:96:74:bc

die IPv6-Adressen

2001:638:404:a800:215:77ff:fe96:74bc
fe80:: 215:77ff:fe96:74bc

Der Router liefert in diesem Fall das IPv6 Subnetz-Prefix und signalisiert per Flag, dass Stateless Address Autoconfiguration (SLAAC) zur Bildung der IPv6-Adresse anzuwenden ist. Für alle Systeme

[9] Extended Unique Identifier (IEEE-Standard)

im lokalen Netz soll jeweils nur eine Global Unicast Adresse und die obligatorische Link Local Adresse gesetzt sein; dies reduziert die Komplexität der Verfahren zur *Source and Destination Address Selection* (RFC3484). Ein Beispiel eines CISCO IOS Routers:

```
interface Vlan12
        ip address 134.94.173.1 255.255.248.0
        ipv6 address FE80::A800:501 link-local
        ipv6 address 2001:638:404:A800::A800:501/64
        ipv6 traffic-filter VLAN12-BLOCK-RFC3041 in
```

Intensiv diskutiert wird der Einsatz sogenannter Privacy Extensions (RFC3041). Dabei werden statt der EUI-64 IIDs zufällige Werte generiert und als IIDs benutzt. Dies ist aus Datenschutzgründen in öffentlichen Netzen (Wifi, Mobilfunk) sicher vorteilhaft, da kein User Tracking über die transformierte MAC-Adresse mehr möglich ist. Jedoch erschwert bzw. behindert im lokalen und zentral administrierten Netzen diese Technik diverse Netzmanagementaufgaben wie DNS Einträge, Firewall-Regeln und Forensik. Linux-Derivate nutzen diese Option derzeit nicht. In den Windows Betriebssystemen und Mac OS X 10.7 sind Privacy Extensions aktiv, sollten aber deaktiviert werden.

Phase 1: IPv6 Testbed - WAN-Anbindung, Firewall, LAN-Routing

Die vorhandenen Router- und Firewall-Plattformen können IPv6 Konnektivität unterstützen. Die Plattformen sind vom Hersteller für einen IPv6 Einsatz im Produktionsbetrieb freigegeben.

Zu Beginn dieser Phase wurde der durch einen CISCO Cat6000 Sup720/MSFC3[10] realisierte Internetzugang nach Zuweisung der Transitnetze durch den Internet-Provider DFN IPv6 fähig gemacht. Die dazu auf dem redundanten Router neu installierte Software *IOS 12.3(33) SXI5 IP Services* hat die benötigte IPv6 Funktionalität. Insbesondere die für einen sicheren Betrieb unverzichtbaren IPv6 Traffic Filter und BGP (Border Gateway Protocol) Security Features sind einsetzbar. Seit der Inbetriebnahme nutzen IPv4 und IPv6 die gleichen Zugangsleitungen – bei Leitungsausfall wird in beiden Fällen das Routing durch den BGP Prozess dynamisch sowohl für IPv4- als auch für IPv6-Traffic umgeschaltet; dabei ist eine Instanz der eingesetzten Multiprotokoll BGP4 (RFC 4760) Implementierung für die IPv4-Routing Einträge und eine weitere für die IPv6-Routing-Einträge zuständig. Die Kommunikation erfolgt dabei im ersten Fall zu den BGP Peer Routern über IPv4 und im zweiten Fall über IPv6. Das für IPv4 bewährte Redundanzkonzept wurde erfolgreich für IPv6 getestet.

Die Fähigkeit der Cisco Adaptive Security Appliance (ASA) IPv6 Traffic zu filtern wurde erstmals mit der Version 7.0 bereitgestellt. Die derzeit in einer redundanten Konfiguration betriebenen Systeme nutzen die Version 8.2(4), die nochmals verbesserte IPv6 Funktionen bereitstellt. Vor der Inbetriebnahme auf dem Produktionssystem wurden in gesonderten Testumgebungen die Einsatzreife im Bereich Basiskonfiguration mit folgenden Aspekten

- IPv6 Interface Konfiguration (manuell Link Local and Global)

[10] Catalyst 6500 mit Supervisor Engine 720 und Multilayer Switch Feature Card 3

- Static Routing
- Router Advertisement

verifiziert.

Folgende spezielle Firewall Funktionen wurden verifiziert:

- IPv6 ACLs und Access Groups
- Koexistenz IPv6 und IPv4 Access Groups
- Stateful Inspection
- IPv6 ICMP
- Stateful Failover
- EUI-64 Enforcement

Für das LAN-Routing ist ebenfalls ein Cat6000 Sup720/MSFC3 im Einsatz. Als Software wird wiederum *IOS 12.2(33) SXI5 IP Services* eingesetzt. IPv6-Routing und Interface-Konfiguration werden auf die Anforderungen in den Subnetzen abgestimmt. Wichtig für die Sicherheit der IOS-Konfiguration ist zudem die Adaption sämtlicher für IPv4 vorhandener Zugangsbeschränkungen auf IPv6 – stellvertretend seien an dieser Stelle die Management-Zugänge (ssh/telnet/https) genannt. IPv6-Routing ist durch statische Einträge konfiguriert. Zur Verkehrsanalyse wird Netflow V9 unterstützt. Dabei werden im Netflow Cache (Policy Feature Card) Statistiken über die Layer 3 Verbindungen (TCP/UDP/ICMPv6) vorgehalten:

```
Router# show mls netflow ipv6 flow [tcp / udp / icmp ]
```

Abschließend wurden sämtliche IPv6-Adressen einem NMAP-SCAN -auch von extern- unterzogen:

```
nmap -6 -sT -PN {ipv6_address}
```

Nach Abschluss der Arbeiten kann für ausgewählte LANs das neue IPv6-Protokoll zur weltweiten Kommunikation bereitgestellt werden. Konzeptionell gibt es dabei keine Unterschiede zu IPv4 bezüglich Verfügbarkeit und Sicherheit.

Phase 2: IPv6 Testbed - Client-Netz (Abt. JSC-KS)

Rund 20 Hosts der Abteilung Kommunikationssysteme wurden in der Phase 2 in einem gesonderten Subnetz durch IPv6 Stateless Address Autoconfiguration mit einer global gültigen IPv6 Adresse versehen. Dabei durchlaufen die LAN-Interfaces bei der Initialisierung nach RFC 2462 folgende Stufen:

- Link-Local Address (EUI-64 IID) generieren
- Neighbor Solicitation (NS) für Duplicate Address Detection (DAD) senden
- Autoconfiguration abbrechen, falls ein Neighbor Advertisement (NA) einen Adresskonflikt anzeigt
- Router Solicitation aussenden
- Falls kein Router Advertisement (RA) empfangen wird, starte DHCPv6
- Falls ein Router Advertisement (RA) empfangen wird:
    - generiere Adressen für die enthaltenen Prefixe; danach DAD
- M Flag == 1 im Router Advertisement (RA):
    - starte DHCPv6 um weitere Adressen und Parameter zu erhalten
- M Flag == 0 und O Flag == 1 im Router Advertisement (RA):
    - starte DHCPv6 um weitere Konfigurationsparameter zu erhalten (z.B. DNS Server)

Als Betriebssysteme waren Windows XP, Windows Vista, Windows 7, Linux und Mac OS X am Test beteiligt; die wesentlichen Merkmale der jeweiligen IPv6 Implementierung zeigt die folgende Aufstellung:

Windows Vista / 7 / 2008

- **IPv6 ist installiert und aktiv**
- Stateless Autoconfiguration aktiv (RFC 2462 / RFC 4862)
- IPv6 Stack: zahlreiche Verbesserungen (Dual Layer)
- GUI, CLI and GPO Konfiguration
- Integrated Internet Protocol security (IPsec) verfügbar
- Privacy Extensions (RFC 3041 /RFC 4941) aktiv
- Domain Name System (DNS) Unterstützung
- Source and Destination Address Selection (RFC 3484)
- DHCPv6 Client aktiv
- Link-Local Multicast Name Resolution (LLMNR)
- Transition Technologies (Tunnel) aktiv
- **Windows Firewall ist IPv6 fähig, Stateful Inspection**

Linux

- **IPv6 ist installiert und aktiv**
- Stateless Autoconfiguration aktiv (RFC 2462 / RFC 4862)
- GUI und CLI Konfiguration möglich
- Privacy Extensions (RFC 3041 / RFC 4941) optional
- Domain Name System (DNS) Unterstützung
- Source and Destination Address Selection (RFC 3484)
- DHCPv6 Client optional
- Multicast DNS
- Transition Technologies (Miredo) optional
- **Firewall: ip6tables, Stateful Inspection ab Kernel 2.6.20**

Mac OS X

- **IPv6 installiert und aktiv**
- Stateless Autoconfiguration (RFC2462 / RFC 4862)
- GUI und CLI Konfiguration möglich
- Privacy Extensions (RFC 3041 / RFC 4941) optional
- ab 10.7 Privacy Extensions aktiv
- Source and Destination Address Selection (RFC3484)
    - Administrative Schnittstelle nicht vorhanden
- DHCPv6 ab 10.7
- Multicast DNS Unterstützung
- Transition Technology (6to4) optional
- **ip6fw – keine grafische Konfigurationsschnittstelle - Standardeinstellung: *accept***

Die Zugriffe nach extern verliefen wie erwartet. Sowohl Windows, Linux und Mac OS X Hosts erreichten die anvisierten Scores auf den einschlägigen Testseiten. Die WAN-Anbindung und die Firewall-Regeln (Stateful Inspection) arbeiteten problemlos. Damit war eine Grundvorrausetzung für den nächsten Skalierungsschritt in Phase 3 erfüllt.

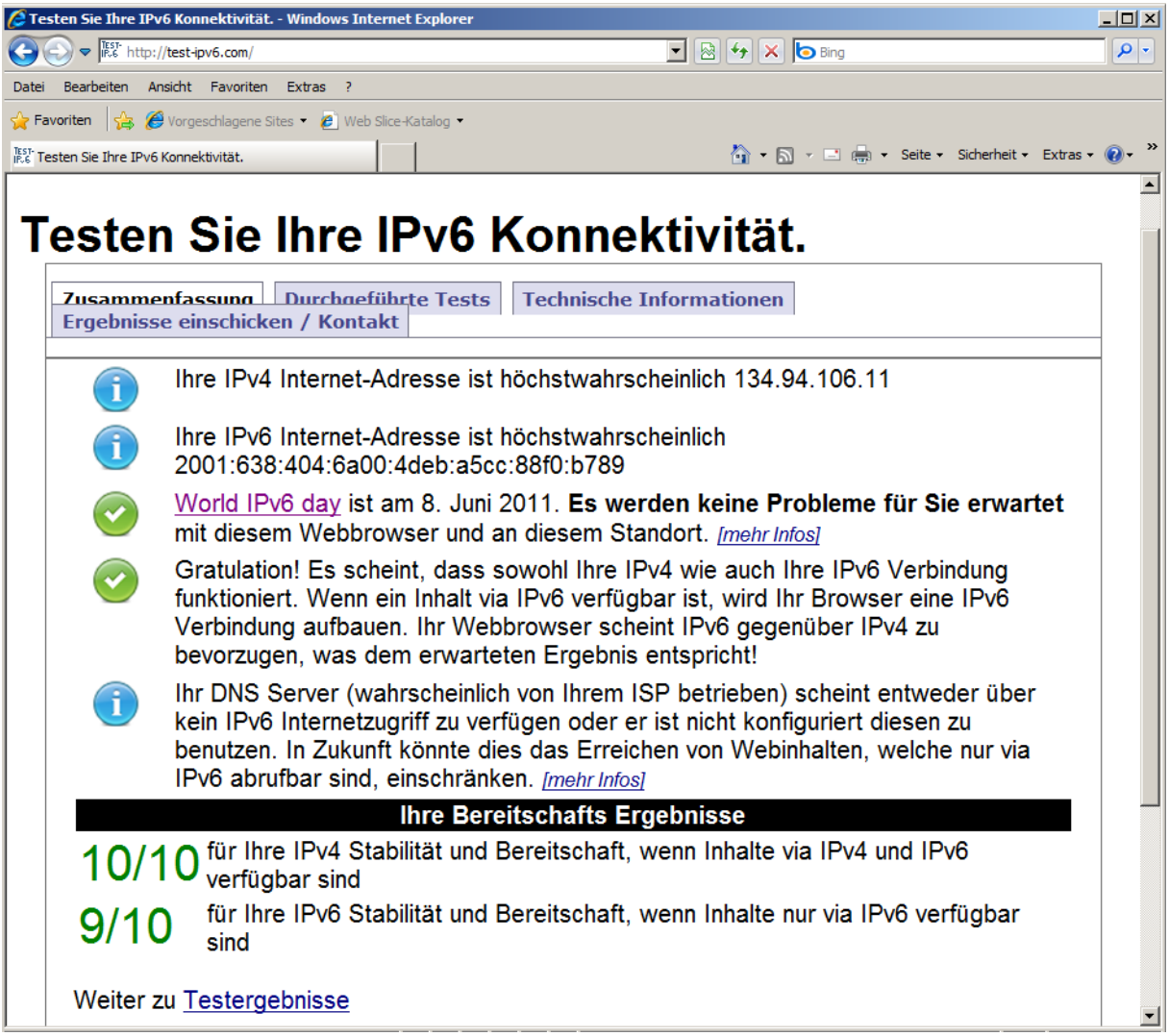
Ohne Anpassung der Voreinstellungen (Auslieferungszustand) der genannten Betriebssysteme zeigen sich abweichende Methoden zur Bestimmung der Interface-Identifier (IID) bei der Initialisierung der IPv6-Module im Kernel und der späteren Autokonfiguration:

IPv6 Interface Identifier	**Link-Local Random**	**Link-Local EUI-64**	**Global Unicast Addr Random**	**Global Unicast Addr Temporary**	**Global Unicast Addr EUI-64**
Windows XP	-	+	-	+	+
Windows 7	+	-	+	+	-
Windows 2008	+	-	+	-	-
Mac OS 10.6	-	+	-	-	+
Mac OS 10.7	-	+	-	+	+
openSUSE 11.3	-	+	-	-	+
Debian 6.0	-	+	-	-	+

Eine Vereinheitlichung auf EUI-64 Interface IDs ist zu favorisieren.

Neben der MAC-Adresse im Fall von EUI-64 Interface IDs lassen sich die folgenden Informationen aus einer Global Unicast Adresse ableiten und bei der Netzwerkdiagnose und Forensik nutzen:

Beispiel - IPv6 Address:	2001:0638:0404:a800:0215:77ff:fe76:74b9	
	Prefix Info	Global Unicast Address (RFC3587) - 2000::/3
	Interface ID Info:	
	IEEE EUI-64 based Interface ID (RFC4291)	
	Hardware Address (IEEE - 48 bit MAC)	00-15-77-76-74-b9
	IPv6 Solicited-Node Multicast Address	ff02::1:ff76:74b9
	Corresponding Ethernet Multicast Address	33-33-ff-76-74-b9
	getaddrinfo Result:	2001:638:404:a800:215:77ff:fe76:74b9



Abschließend konnten Konfigurationsempfehlungen für die Phase 3 ausgearbeitet und getestet werden.

Phase 3: IPv6 Testbed - Client-Netz (JSC weit)

Die Mechanismen zur Autokonfiguration und verschiedene Sicherheitseinstellung sollten in der Phase 3 für eine größere Anzahl Hosts im Dual Stack Betrieb getestet werden. Zudem sollten Mechanismen für das EUI-64 Enforcement erprobt werden. Das IPv6-Protokoll sollte als Zusatz im Workstation-Netz im JSC angeboten werden, d.h. IPv6-fähige Systeme in diesem Subnetz erhalten zusätzlich zur gewohnten IPv4-Adresse eine IPv6-Adresse. Die IPv6 Konfiguration der IPv6-Adresse erfolgt automatisch durch Stateless Address Autoconfiguration (SLAAC). Die Auswertung der Netzstatistiken wies auf mehr als **400 Systeme** mit aktiviertem IPv6 hin – u.a. erkennbar an der IPv6 Link Local Multicast Kommunikation. Sobald der Router das entsprechende IPv6-Prefix bekannt gibt, sollten folglich diese Systeme im Dual Stack Betrieb die Kommunikation über IPv6 bevorzugen (RFC 3484).

Die Systemadministratoren konnten zwischen folgenden Varianten mit den entsprechenden Handlungsanweisungen wählen:

Fall A) Nicht am IPv6 Test teilnehmen und IPv6 im LAN deaktivieren:

openSuse 11.x	YAST – Network Devices –> Network Settings -> Global Options -> enable ipv6 abwählen und danach REBOOT
Windows Vista/7/2008	Systemsteuerung -> Netzwerk- und Freigabecenter ->LAN-Verbindung -> Internet Protokoll Version 6 (TCP/IPv6) abwählen
MAC OS X	sudo ip6 -x

Fall B) Am IPv6 Test teilnehmen:

Für Windows 7/Vista/2008 System sind dabei folgende Einstellungen und Empfehlungen zu befolgen. Die Adressen der IPv6 Autokonfiguration müssen mit den bekannten Hardware-Adressen der JuNet-Datenbank synchron sein - dazu bitte als **Administrator** folgende Befehle ausführen:

```
netsh interface ipv6 set privacy state=disabled  store=persistent
netsh interface ipv6 set global  randomizeidentifiers=disabled  store=persistent
```

und Neustart

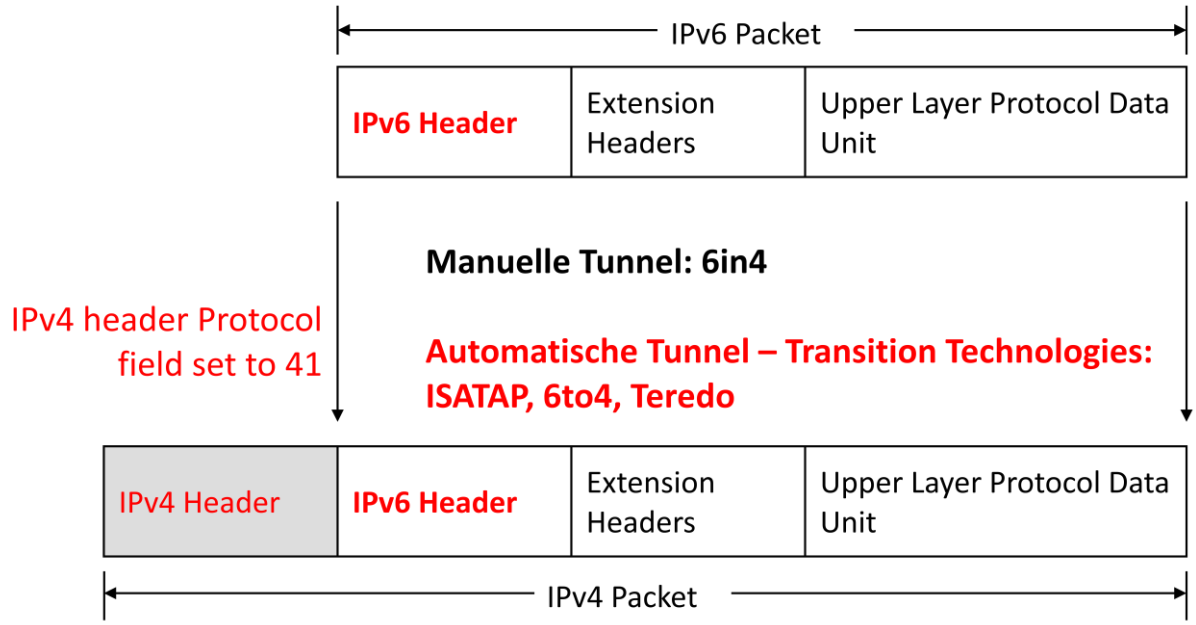
Ab Mac OS X 10.7 sind Privacy Extensions aktiv und müssen abgeschaltet werden. Die Datei /etc/sysctl.conf muss folgende Zeile enthalten:

```
net.inet6.ip6.use_tempaddr=0
```

und Neustart

Die Betriebssysteme Windows Vista/7/2008 versuchen automatisch IPv6-Tunnel zu starten. Dieser Mechanismus ist unabhängig von den IPv6 LAN-Einstellungen (Fall A). Also: Auch bei deaktiviertem IPv6 für die LAN Anbindung sind die Tunnel aktiv!

Generell gilt, dass dies keine Besonderheit der Netzkonfiguration im FZJ ist. Wird ein derartiger Tunnel aktiv, ist das System als IPv6 Ziel erreichbar. Es wird daher empfohlen, diese Tunnel abzuschalten - insbesondere auf Laptops.



… aber auch Varianten mit GRE, IPSEC oder UDP Encapsulation

IPv6 Tunnel Encapsulation

Der **System-Administrator** führt zum Abschalten der Tunnel folgende Befehle aus:

netsh interface ipv6 6to4 set state disabled undoonstop=disabled

netsh interface ipv6 isatap set state disabled

netsh interface ipv6 set teredo disable

und Neustart

Falls die Windows Systeme Mitglied einer Domäne (Active Directory) sind, können die Einstellungen zentral verwaltet werden (AD GPO):

Computer Configuration > Policies

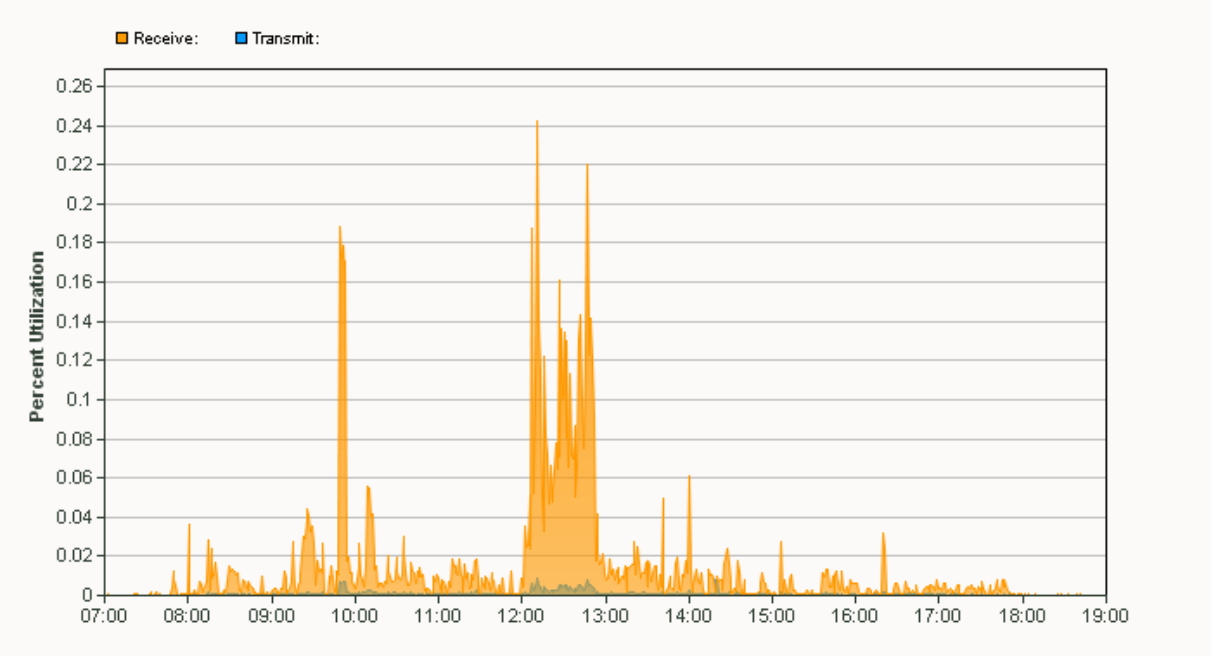
> Administrative Templates > Network > IPv6 Configuration

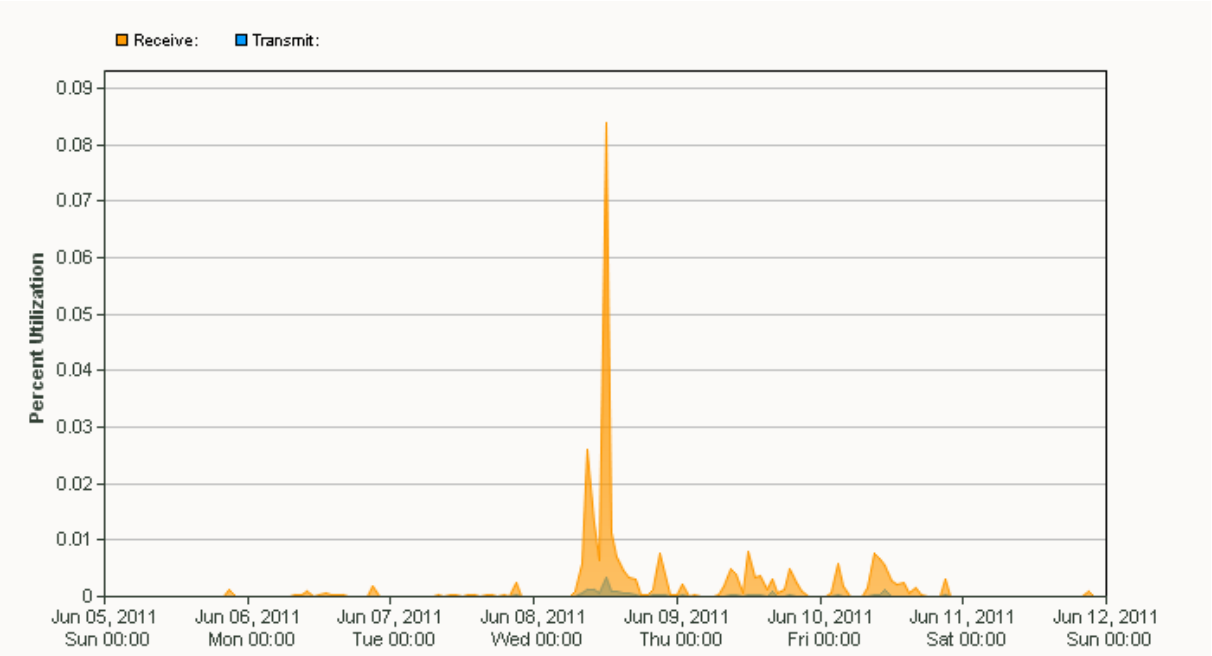
Mögliche Pv6 Einstellungen:

Enable all IPv6 components (Windows default)
Disable all IPv6 components
Disable 6to4
Disable ISATAP
Disable Teredo
Disable Teredo and 6to4
Disable all tunnel interfaces
Disable all LAN and PPP interfaces
Disable all LAN, PPP and tunnel interfaces
Prefer IPv4 over IPv6.

Da fast alle Systeme aktiv im Testbed mitliefen (Fall B), wurde beim IPv6 **Test Day am 8. Juni** erwartungsgemäß ein erhöhtes IPv6-Verkehrsaufkommen gesehen. Seit dem 8. Juni hat das Volumen sichtbar zugenommen.

IPv6 Test Day – 8. Juni 2011





Das EUI-64 Enforcement wurde nach dem IPv6-Day über einen Interface-spezifischen Traffic Filter auf dem Router implementiert und aktiviert. Dabei werden nur Interface Identifiers mit gesetztem U/L-Bit erlaubt. Die Liste zeigt die möglichen Muster:

::x2:xx:xx:xx:xx:xx

::x6:xx:xx:xx:xx:xx

::xA:xx:xx:xx:xx:xx

::xE:xx:xx:xx:xx:xx

Eine entsprechende IPv6 Access Control List (ACL) muss pro Subnetz erstellt werden, um nur zulässige Kombinationen weiterzuleiten. Hier ein Beispiel für eine solche Interface-ACL, die auf einem Router Interface wirkt:

```
ipv6 access-list VLAN12-BLOCK-RFC3041
        remark Block randomized and temporary IPv6 addresses from routing core
        deny     any  fec0::/10
        deny     any  fd00::/7
        permit   2001:0638:0404:a800:0000::/80 any
        permit   2001:0638:0404:a800:0200::/72 any
        !!!  Alle möglichen Kombinationen auflisten
                  .....
                  .....
        permit   2001:0638:0404:a800:fe00::/72 any
        deny     2001:0638:0404::/48  any   log
        permit   any any
        remark   NOW IMPLICIT DENY / icmpv6 ND allowed
        end
```

Im Bereich der Personal Firewall bleibt die Empfehlung bestehen, die Microsoft-Firewall, die sowohl IPv4 als auch IPv6 Stateful Inspection bietet und die Transition Technologies korrekt behandelt, zu benutzen. Personal Firewalls verschiedener Hersteller zeigen im Umgang mit IPv6 wenig Überzeugendes. Insbesondere die Behandlung von Tunnel-Protokollen zeigte sich bei Tests unzureichend. Linux-Administratoren können ab Kernel 2.6.20 mit ip6tables ebenfalls eine Stateful Inspection konfigurieren:

```
# Generated by ip6tables-save v1.4.10 on Tue May 24 13:40:49 2011
*filter
:INPUT DROP [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
## Accept incoming traffic on loopback
-A INPUT -i lo -j ACCEPT
##
## Accept SSH from local subnet
-A INPUT -s fe80::/64 -i eth0 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 2001:638:404:a800::/64 -i eth0 -p tcp -m tcp --dport 22 -j ACCEPT
## Accept ICMPv6 from local-link
-A INPUT -s fe80::/64 -i eth0 -p icmpv6 -j ACCEPT
-A INPUT -s 2001:638:404:a800::/64 -i eth0 -p icmpv6 -j ACCEPT
## Load state module
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Tue May 24 13:40:49 2011
```

Auf Layer 2 wurde zur Erhöhung der Betriebssicherheit erstmals auf den neu eingesetzten CISCO Cat 4500 Sup 7[11] Switches auf allen Access-Ports eine IPv6-Port-ACL geschaltet, die Rogue Router und Rogue DHCPv6 Advertisements sperrt:

```
IPv6 access-list BlockRA
        deny icmp any any router-advertisement log sequence 10
        deny udp any eq 547 any eq 546 log sequence 20
        permit ipv6 any any  sequence 30


interface FastEthernet1/11
        !! Beispiel-Port – Layer 2
         switchport access vlan nn
         switchport mode access
                  ……
        ipv6 traffic-filter BlockRA in
        end
```

Der ‚RFC 6104 – Rogue IPv6 RA Statement' liefert eine umfassende Zusammenstellung der Problematik.

[11] Catalyst 4500 Supervisor Engine 7

Phase 4: IPv6 Testbed - Server-Netz

Die Phase 4 sollte sowohl neben der manuellen Konfiguration von Servern in einem separaten Subnetz mit festen IPv6-Adressen die Überwachung der IPv6 Umgebung inklusive Services auf Produktionsniveau anheben. Entscheidend an dieser Stelle ist das Zusammenspiel von Konfiguration des IPv6 Hosts, DNS Infrastruktur mit DNS AAAA Records für die Server in der Forward Lookup Zone und die lokalen Sicherheitseinstellungen in Personal Firewall Profilen oder Wrappern. Erhält ein Client bei der DNS-Anfrage zu einem Server-Namen sowohl einen A-Record (IPv4 Address Record) als auch einen AAAA-Record (IPv6 Address Record) als Antwort, bevorzugt der Client nach RFC 3484 das neue IPv6 Protocol. Vorrausetzung ist natürlich wie im JSC Workstation-Netz, dass eine routbare IPv6 (Global Unicast oder ULA) konfiguriert ist, die der Client als Absenderadresse nutzen kann. Der im JSC eingesetzte DNS Server (Bind 9) ist IPv6 fähig.

Der Server für die Netzüberwachung wurde konfiguriert und prüft die Verbindung zu den benannten IPv6 Gegenstellen im X-WiN, die eigenen Transportnetze zwischen Routern und Firewall sowie den für IPv6-Nutzung konfigurierten Terminal- und File-Server. Daneben wurden im Workstationnetz ebenfalls diverse Arbeitsplatzrechner mit DNS AAAA Records versehen. Seitdem laufen in diesem Netz die SSH-Zugriffe, Remote Desktop-Sitzungen oder beispielsweise der Zugriff auf Dateifreigaben dieser Hosts automatisch über IPv6. Nochmals sei herausgestellt, dass die Router Advertisement (RA) auf diese Art der Host Konfiguration im Server-Netz explizit abgestimmt sind und kein Stateless Address Autoconfiguration (SLAAC) Flag gesetzt haben (RFC 4861 – Neighbor Discovery for IPv6). Zwar existieren Möglichkeiten für die unterschiedlichen Betriebssysteme, SLAAC zu deaktivieren oder RAs in der Personal Firewall zu filtern, jedoch sind diese nicht einheitlich und kaum verifiziert.

SLAAC kann in den Microsoft Windows Betriebssystemen pro Netzwerkadapter wie folgt deaktiviert werden:

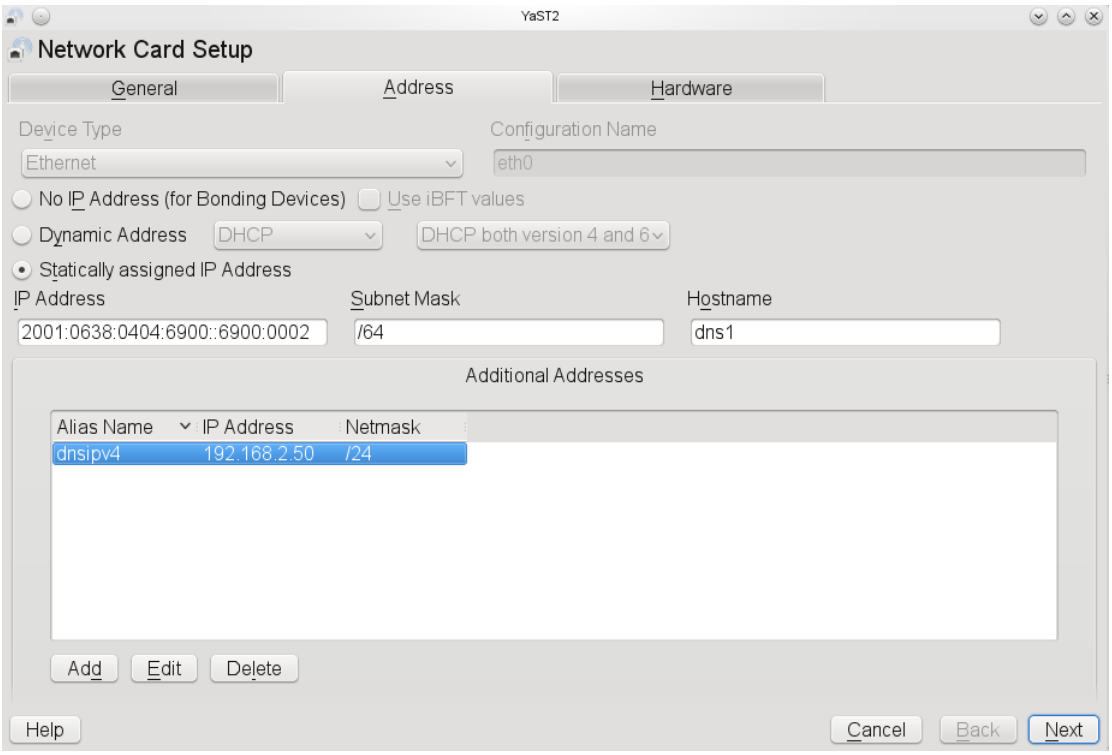
```
netsh interface ipv6 set interface „IfIndex“ routerdiscovery=disabled

netsh interface ipv6 set interface „IfIndex“ routerdiscovery=disabled store=persistent
```

Linux-Administratoren können im Bedarfsfall die Autokonfiguration eines Netzwerkadapters, hier im Beispiel eth0, durch einen Eintrag in die /etc/sysctl.cnf deaktivieren:

```
net.ipv6.conf.eth0.autoconf = 0
```

Das folgende Beispiel aus einer Test-Umgebung zeigt einen openSuse 11.3 Host, der manuell mit einer festen IPv6-Adresse und einer aus einem Rogue-Router-Advertisement bestimmten IPv6-Adresse kommuniziert – dieser Zustand ist unbedingt zu vermeiden. Router Advertisements und deren Kontrolle (RA-Guard) müssen mit der Host-Konfiguration Hand-in-Hand gehen.




```
dns1:~ # ifconfig  -a
eth0      Link encap:Ethernet  HWaddr 00:0C:29:2D:35:25
          inet6 addr: 2001:470:1f0a:1c1f:20c:29ff:fe2d:3525/64 Scope:Global
          inet6 addr: fe80::20c:29ff:fe2d:3525/64 Scope:Link
          inet6 addr: 2001:638:404:6900::6900:2/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:41 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1589 (1.5 Kb)  TX bytes:14745 (14.3 Kb)
          Interrupt:19 Base address:0x2024

eth0:dnsi Link encap:Ethernet  HWaddr 00:0C:29:2D:35:25
          inet addr:192.168.2.50  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:19 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:72 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4960 (4.8 Kb)  TX bytes:4960 (4.8 Kb)

dns1:~ #
```

Zur Absicherung anderer Broadcast Domains, insbesondere solcher, die derzeit nur IPv4 Funktionalität haben, wurde ein NDPMON[12]-Server installiert, der eine Historie über die Zuordnung von RFC3041 IPv6 Adressen und MAC-Adressen liefert sowie über Rogue Router Advertisements informiert. Als Rogue Router traten bisher in der Regel Windows Rechner mit aktivem Internet Connection Sharing (ICS) in Erscheinung.

[12] Neighbor Discovery Protocol Monitor

Phase 5: IPv6 Testbed - Fazit - IPv6 Zukunft im Forschungszentrum

Im Zeitraum von März 2011 bis September 2011 wurde die IPv6 Nutzung im JSC sukzessive durch Ausbau und Beteiligung weiterer Komponenten gesteigert. Festzuhalten bleibt, dass es keine unvorhergesehenen Nebeneffekte oder gar Fehler durch den Dual Stack Betrieb der Client- und Server-Systeme in den jeweiligen Subnetzen im JSC gegeben hat. Die Routing- und Firewall-Plattformen haben während dieser Zeit stabil am Testbed teilgenommen; Rekonfigurationen oder ein Neudesign waren in keinem Teilbereich nötig.

Der IPv6-Adressplan hat sich in der Praxis bewährt und kann flächendeckend im lokalen Netz und in den Außenstellen zur Anwendung kommen.

Wichtig ist jedoch eine klare Strukturierung im lokalen Netz. Mechanismen aus der IPv4 Welt wie logisches Subnetze wirken kontraproduktiv und müssen vor der IPv6 Einführung konsolidiert werden. Im strukturierten lokalen Netz kann danach wie in Phase 3 beschrieben vorgegangen werden.

Der Aufwand zur Anpassung von Management-Software und Datenbank-Tools ist eher einmalig, im laufenden Betrieb ergibt sich kein unkalkulierbarer Mehraufwand; hierbei ist jedoch insbesondere nochmals auf das unabdingbare Training der Netzwerkspezialisten im Umgang mit dem neuen Protokoll zu verweisen. Dies offeriert den Weg zur proaktiven Integration dieser Netzwerktechnik in das lokale Netz und die spätere effiziente und zielgenaue Unterstützung von Anwendungen.

Falls für Applikationen mit hoher Außenwirksamkeit wie EMAIL oder WWW zukünftig die Erreichbarkeit über IPv6 gewünscht wird, kann auf ein erprobtes IPv6 Core-Netzwerk mit WAN-Anbindung zurückgegriffen werden. Die in Phase 4 erprobte Netzwerkkonfiguration beschreibt dieses Szenario. Diese Applikationen verlangen jedoch weitere spezifische Betrachtungen im Detail. Dazu gehören u.a. die Anpassung und Vorbereitung der Reverse-DNS-Zonen oder im WWW-Fall der Einsatz IPv6-fähiger Load-Balancer.

In den Außenstellen kann im Bedarfsfall ebenfalls IPv6 bereitgestellt werden. Die zur sicheren Anbindung dieser Standorte konfigurierten GRE/IPSEC-Tunnel transportieren sowohl IPv4 als auch bei Bedarf IPv6 Payload. Für die LAN-Umgebung gelten die Randbedingungen des Campusnetzes in Jülich. Das Szenario wurde in einer gesonderten Labor-Umgebung getestet.

Im Bereich der Access-VPNs sind die Microsoft VPN Lösungen L2TP/IPSEC[13] und IKEv2[14] in der Lage, sowohl IPv6 Payload als auch IPv6 Transport zu unterstützen. Ab Windows 2008 X 2 als VPN-Gateway und der OpenSource Implementierung Freeradius 2.x werden die IPv6-Attribute Prefix und Interface-ID korrekt im Accounting festgehalten. Diese Funktionen wurden ebenfalls in einer Testumgebung untersucht. Die Cisco-VPN-Lösungen unterstützen zurzeit noch keinen IPv6 Transport (äußerer Tunnel).

[13] Layer 2 Tunneling Protocol / Internet Protocol Security
[14] Internet Key Exchange V2

Anhang – IPv6 Tests im JSC Labor

In gesonderten Testumgebungen wurden gezielt Teilfunktionen des neuen Protokolls getestet um deren Bedeutung im realen Einsatz abwägen zu können.

Als Routing-Protokolle wurden im LAN als Alternative zum eingesetzten statischen Routing die Protokolle **OSPFv3**[15] und **RIPng**[16] getestet. Beide Protokolle transportieren ausschließlich Routing-Informationen für IPv6:

```
ipv6 router ospf 1
        router-id 192.168.2.40  !! muss eine 32 Bit Zahl sein (a.b.c.d Format)
        log-adjacency-changes
        passive-interface Vlan101
        passive-interface Vlan102
        passive-interface Vlan103
        maximum-paths 4
```

Optimale Sicherheit dieser dynamischen Routing-Protokolle kann nur in Verbindung mit IPSEC gewährleistet werden. Aufgrund des daraus resultierenden Overheads und der überschaubaren LAN-Struktur werden diese Protokolle vorerst nicht eingesetzt.

Als Alternative zur Stateless Address Autoconfiguration (SLAAC) wurde **DHCPv6** untersucht. Die eingesetzten CISCO Router können als Relay arbeiten und insbesondere auch als Stateless DHCPv6 Server agieren. Dieser **Stateless DHCPv6** Betrieb ist insbesondere in reinen IPv6 Netzen von besonderem Vorteil, weil so auf einfache Art die notwendigen DNS-Parameter als Ergänzung zur Stateless Address Autoconfiguration verteilt werden können.

```
ipv6 dhcp pool IPV6ONLY
        dns-server 2001:638:404:6900::6900:2
        domain-name example.com
……..

interface Vlan101
        description Client hosts - SLAAC + Stateless DHCP
        no ip address
        no ip proxy-arp
        ipv6 address 2001:638:404:6800::6800:1/64
        ipv6 address FE80::6800:1 link-local
        ipv6 enable
        ipv6 nd ra-interval 20
        ipv6 nd other-config-flag
        ipv6 dhcp server IPV6ONLY
        ipv6 ospf 1 area 52425
```

[15] Open Shortest Path First
[16] Routing Information Protocol next generation

Stateful DHCPv6 wurde sowohl mit der ISC Server Implementierung als auch mit der Windows 2008 Implementierung getestet. Die Vergabe von IPv6-Adressen aus dynamischen Bereichen funktioniert; die feste Vergabe von Adressen setzt allerdings die Verwaltung und Zuordnung der DUIDs (DHCPv6 Unqiue Identifier) zu IPv6-Adressen voraus. Leider unterstützen nicht alle Client Hosts DHCPv6 und im Linux-Umfeld erwies sich die Integration in die Distributionen als störanfällig. Zur Verdeutlichung hier die Anzeige des DUID für Windows und Linux sowie die mit Wireshark aufgezeichnete DHCP-Solicitation des LINUX-Rechners:

```
Ethernet-Adapter VMware Network Adapter VMnet1:

   Verbindungsspezifisches DNS-Suffix:
   Beschreibung. . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet1
   Physikalische Adresse . . . . . . : 00-50-56-C0-00-01
   DHCP aktiviert. . . . . . . . . . : Nein
   Autokonfiguration aktiviert . . . : Ja
   Verbindungslokale IPv6-Adresse  . : fe80::250:56ff:fec0:1%13(Bevorzugt)
   IPv4-Adresse  . . . . . . . . . . : 192.168.40.1(Bevorzugt)
   Subnetzmaske  . . . . . . . . . . : 255.255.255.0
   Standardgateway . . . . . . . . . :
   DHCPv6-IAID . . . . . . . . . . . : 335564886
   DHCPv6-Client-DUID. . . . . . . . : 00-01-00-01-12-FD-AA-28-00-15-77-76-74-B9
```

```
linux-cjsj:/var/lib/dhcp6 #
linux-cjsj:/var/lib/dhcp6 # cat dhclient6.eth0.lease
default-duid "\000\001\000\001\026\004\333\337\000\014)\311\020\275";
linux-cjsj:/var/lib/dhcp6 #
```

```
▼ DHCPv6
    Message type: Solicit (1)
    Transaction ID: 0x786ac4
  ▼ Client Identifier: 000100011604dbdf000c29c910bd
      Option: Client Identifier (1)
      Length: 14
      Value: 000100011604dbdf000c29c910bd
      DUID type: link-layer address plus time (1)
      Hardware type: Ethernet (1)
      Time: Sep 15, 2011 17:53:03 CEST
      Link-layer address: 00:0c:29:c9:10:bd
  ▶ Option Request
  ▶ Elapsed time
  ▶ Identity Association for Non-temporary Address
```

Die DHCPv6 Solicitation kann beispielsweise durch folgende IOS-Konfiguration zu einem entfernten DHCPv6 Server transportiert werden:

```
interface Vlan103
    description Client EUI-64 Hosts - no SLAAC + Statefull DHCPv6 (Linux)
    no ip address
    no ip proxy-arp
    ipv6 address 2001:638:404:A802::A802:1/64
    ipv6 address FE80::A801:2 link-local
```

```
ipv6 enable
ipv6 nd ra-interval 10
ipv6 nd prefix 2001:638:404:A802::/64 2592000 604800 no-autoconfig
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp relay destination 2001:638:404:6900::6900:2
ipv6 ospf 1 area 52425
```

Die Anbindung über Tunnelbroker wie **SixXS** und **Hurricane Electric** wurde in Verbindung mit Fragestellungen zur Source and Destination Address Selection (RFC 3484) im Vergleich zu **6to4** untersucht. Als Transport wurde AYIYA (Anything in Anything) sowie 6in4 genutzt. Hier zeigte sich die Bedeutung der Prefix Policy Table bei der Auswahl des Transportprotokolls abhängig von der Tunnelvariante: Im Fall der Transition Technology 6to4 bewirkt das eigene Label in der Prefix Policy Table beispielsweise eine Bevorzugung von IPv4 als natives Protokoll, wenn das Zielsystem (Internet) nicht im Bereich des Prefix 2002::/16 (6to4 Tunnel Prefix) liegt. Lokal im Forschungszentrum wird 6to4 gegenüber IPv4 bevorzugt. Die Prefix Policy Table eines Windows 7 Rechners:

```
C:\>netsh int ipv6  show   prefixpol
        Der aktive Status wird abgefragt...

Vorgänger   Label       Präfix
----------      -----       --------------------------------
50              0       ::1/128
40              1       ::/0
30              2       2002::/16
20              3       ::/96
10              4       ::ffff:0:0/96
5               5       2001::/32
```

IPSEC gesicherte Kommunikation zum Transport von IPv6 wurde ebenfalls in Verbindung mit GRE (Generic Routing Encapsulation) geprüft. Als Payload wird dabei sowohl IPv4 als auch IPv6 komplett verschlüsselt. Ein Konfigurationsbeispiel:

```
crypto isakmp policy 10
        encr 3des
         hash md5
        authentication pre-share
        crypto isakmp key PresharedKeyString address 192.168.3.2
!
crypto ipsec transform-set GEHEIM esp-3des esp-sha-hmac
!
crypto map SCHUTZ 10 ipsec-isakmp
        set peer 192.168.3.2
        set transform-set GEHEIM
        match address VPN-TRAFFIC
!
```

```
……..
interface Tunnel1
        description GREoverIPSEC Tunnel - forward IPv4 + IPv6
        ip address 192.168.4.1 255.255.255.0
        ipv6 address 2001:638:404:6F01::6F01:1/126
        ipv6 enable
        ipv6 ospf cost 1
        ipv6 ospf 1 area 52425
        tunnel source 192.168.3.1
        tunnel destination 192.168.3.2
!
interface Vlan104
         ip address 192.168.3.1 255.255.255.0
         no ip proxy-arp
         crypto map SCHUTZ
!
……

!
ip access-list extended VPN-TRAFFIC
        permit gre host 192.168.3.1 host 192.168.3.2
!
```

Reverse DNS für IPv6 konnte für die aktuell eingesetzte ISC Bind Version 9.7.x auf einem Suse Linux Rechner im Test-Labor verifiziert werden. Für die Rückwärtsauflösung ist die Definition einer neuen Zone unterhalb **4.0.4.0.8.3.6.0.1.0.0.2.ip6.arpa** nötig. Hier als Beispiel ein Reverse DNS-Request:

Linux: nslookup 2001:638:404:4711::500

Server: 127.0.0.1
Address: 127.0.0.1#53

0.0.5.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.7.4.4.0.4.0.8.3.6.0.1.0.0.2.ip6.arpa name = ikev2.jsc.kfa-juelich.de.

Literatur

[1] IPv6 Security – Protection measures for the next Internet Protocol; E. Vyncke; Cisco Press; ISBN-13 978-1-58705-594-2

[2] Understanding IPv6; J. Davies; Microsoft Press; ISBN-13 978-0-7356-2446-7

[3] IPv6 for Enterprise Networks; S. McFarlan et al.; Cisco Press; ISBN-13: 978-1-58714-227-7

[4] Requirements for IPv6 in ICT Equipment; J. Zorz, S. Steffann

[5] IPv6 Stateless Address Autoconfiguration; RFC2462 / RFC 4862

[6] Rogue IPv6 Router Advertisement Problem Statement; RFC 6104

[7] IP Version 6 Addressing Architecture; RFC 4291

[8] Connection of IPv6 Domains via IPv4 Clouds; RFC3056

[9] IPv6 Unicast Address Assignment Considerations; RFC 5375

[10] Address Allocation for Private Internets; RFC 1918

[11] Unique Local IPv6 Unicast Addresses; RFC 4193

[12] Dynamic Host Configuration Protocol for IPv6 (DHCPv6); RFC 3315

[13] Default Address Selection for Internet Protocol version 6 (IPv6); RFC 3484

[14] Privacy Extensions for Stateless Address Autoconfiguration in Ipv6; RFC 3041/RFC 4941

[15] Multiprotocol Extensions for BGP-4; RFC 4760

[16] IPv6 Global Unicast Address Format; RFC 3587

[17] Neighbor Discovery for IP version 6 (IPv6); RFC 4861